Scalable Intrusion Detection for the Emerging Network
"JiNao Report"

'203 Claim number	Claim Term	JiNao Report (printed publication)
		"3.2 Scalability Even though the current scope of the project focuses on the development of local detection capabilities, we expect the system design can be easily extended to a regional and even a more global level. While it is not within the scope of this project, we expect the detection/analysis functions implemented in the local subsystem can be extended to a global level and correlate intrusion events among several routers. The extension to a global level can be hierarchical where several regional management stations can aggregate their detection information to a higher level for establishing a global view of the routing domain status. The communication of this extension can be provided through SNMP ManagerToManager operations." (13) [SYM_P_0070558] "While it is more efficient to detect intrusions locally, as far as possible, there are cases where only a global agent can make a determination of whether an intrusion has taken place based on information gathered from several local JiNao decision modules." (29) [SYM_P_0070574] "The fact that the local decision module uses information disseminated by the remote JiNao agents in order to make a decision on intrusion leads to a scalable architecture. Indeed, in the converse situation, if the local agents had to forward all their detection information to the global agent in order for the global agent to make the decision, the global agent would become the centralized decision maker and the architecture would not scale. In our system global information is utilized locally to make a globally aware local decision regarding intrusion. Moreover, the architecture also provides for monitoring attacks which can only be detected at a higher network level." (31) [SYM_P_0070576] "Scope of impact information is used by a set of distributed JiNao decision modules in order to better enhance the accuracy of intrusion detection decisions. For example, ... a higher-level decision module, i.e. one that has access to observations on a larger topological region, can correlate multiple detections from low-levels according to their respective scope of impact, and to reach a more accurate detection decision." (32) SYM_P [SYM_P_0070577]
8	The method of claim 7, wherein receiving and	"The management capability, which is based on SNMP framework, can logically be further extended among management nodes in a hierarchical fashion to establish a status map for an autonomous system." (3) [SYM_P_0070548]

Scalable Intrusion Detection for the Emerging Network
"JiNao Report"

'203' Claim number	Claim Term	JiNao Report (printed publication)
	integrating is performed by a domain monitor with respect to a plurality of service monitors within the domain monitor's associated network domain.	"**2.2.2 Remote Subsystem** In the current scope of the project, a remote subsystem consists of a set of management applications for monitoring and controlling a few local detection subsystems. It is expected that a management application would be able to re-configure the local detection system dynamically. With this configurability, the local detection subsystem can respond to intrusion differently under different situations. Ideally, as a natural extension of the current scope of the project, we expect that a remote subsystem can also implement similar detection capabilities in order to detect a larger scale of orchestrated attack. We realize that some attacks (for instance, door-knob rattling attack) can only be detected on a more global scale. One approach in dealing with these attacks is for the management applications to communicate with their local detection agents in order to form a global view of the domain surrounding this remote subsystem. The notion of global detection can be further extended to cover more than one remote subsystem, either in a distributed or hierarchical fashion. ... Two or more remote subsystems can establish a global view of the network by exchanging detection information from their domains. If the remote subsystems are organized in a distributed fashion, the communication among them is through manager to manager operation. Otherwise, the communication will be manager to agent operation when the system is in a hierarchical architecture." (6-7) [SYM_P_0070551- SYM_P_0070552] "**3.2 Scalability** Even though the current scope of the project focuses on the development of local detection capabilities, we expect the system design can be easily extended to a regional and even a more global level. While it is not within the scope of this project, we expect the detection/analysis functions implemented in the local subsystem can be extended to a global level and correlate intrusion events among several routers. The extension to a global level can be hierarchical where several regional management stations can aggregate their detection information to a higher level for establishing a global view of the routing domain status. The communication of this extension can be provided through SNMP ManagerToManager operations." (13) [SYM_P_0070558] "While it is more efficient to detect intrusions locally, as far as possible, there are cases where only a global agent can make a

Scalable Intrusion Detection for the Emerging Network "JiNao Report"

'203 Claim number	Claim Term	JiNao Report (printed publication)
		determination of whether an intrusion has taken place based on information gathered from several local JiNao decision modules." (29) [SYM_P_0070574] "The fact that the local decision module uses information disseminated by the remote JiNao agents in order to make a decision on intrusion leads to a scalable architecture. Indeed, in the converse situation, if the local agents had to forward all their detection information to the global agent in order for the global agent to make the decision, the global agent would become the centralized decision maker and the architecture would not scale. In our system global information is utilized locally to make a globally aware local decision regarding intrusion. Moreover, the architecture also provides for monitoring attacks which can only be detected at a higher network level." (31) [SYM_P_0070576] "Scope of impact information is used by a set of distributed JiNao decision modules in order to better enhance the accuracy of intrusion detection decisions. For example, ... a higher-level decision module, i.e. one that has access to observations on a larger topological region, can correlate multiple detections from low-levels according to their respective scope of impact, and to reach a more accurate detection decision." (32) SYM_P_[SYM_P_0070577]
9	The method of claim 1, wherein deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 8
11	The method of claim 9,	"Figure 1: Ji-Nao System Architecture" "ManagerToManager" (4) [SYM_P_0070549]

Scalable Intrusion Detection for the Emerging Network
"JiNao Report"

'203 Claim number	Claim Term	JiNao Report (printed publication)
	wherein the plurality of domain monitors within the enterprise network establish peer-to-peer relationships with one another.	"**2.2.1.4 Local Decision Module** ... Through both local and remote MIB agents, the decision module provides its local view of neighbor status to remote management applications for identifying any global scale of attacks. It also relays commands from remote management applications for identifying any global scale of attacks. It also relays commands from remote management applications to the local prevention module and detection modules." (6) [SYM_P_0070551] **2.2.2 Remote Subsystem** ...One approach in dealing with these attacks is for the management applications to communicate with their local detection agents in order to form a global view of the domain surrounding this remote subsystem. The notion of global detection can be further extended to cover more than one remote subsystem, either in a distributed or hierarchical fashion. **2.2.2 Management Information Exchange Protocol** The management information exchange protocol (*e.g.* SNMP) provides communication channels between remote management applications and local MIB agents (manager to agent) or between any pair of remote subsystems (manager to manager).... Two or more remote subsystems can establish a global view of the network by exchanging detection information from their domains. If the remote subsystems are organized in a distributed fashion, the communication among them is through manager to manager operation." (6-7) [SYM_P_0070551- SYM_P_0070552]
12	An enterprise network monitoring system comprising:	See '203 claim 1
	a plurality of network monitors deployed within an enterprise network;	See '203 claim 1
	said plurality of network monitors detecting suspicious network activity	See '203 claim 1

Scalable Intrusion Detection for the Emerging Network "JiNao Report"

'203 Claim number	Claim Term	JiNao Report (printed publication)
	based on analysis of network traffic data selected from the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet};	
	said network monitors generating reports of said suspicious activity; and	See '203 claim 1
	one or more hierarchical monitors in the enterprise network, the hierarchical monitors adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 1
13	The system of claim 12,	See '203 claim 2

Scalable Intrusion Detection for the Emerging Network "JiNao Report"

'203 Claim number	Claim Term	JiNao Report (printed publication)
	wherein the integration comprises correlating intrusion reports reflecting underlying commonalities.	
14	The system of claim 12, wherein the integration further comprises invoking countermeasures to a suspected attack.	See '203 claim 3
15	The system of claim 12, wherein the plurality of network monitors include an application programming interface (API) for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4
16	The system of claim 12, wherein the enterprise network is a TCP/IP network.	See '203 claim 5
17	The system of claim 12, wherein the network	

Scalable Intrusion Detection for the Emerging Network "JiNao Report"

'203 Claim number	Claim Term	JiNao Report (printed publication)
	monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	
18	The system of claim 12, wherein the plurality of network monitors includes a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 8
19	The system of claim 18, wherein a domain monitor associated with the plurality of service monitors within the domain monitor's associated network domain is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 8
20	The system of claim 12, wherein the plurality of	See '203 claim 9

Scalable Intrusion Detection for the Emerging Network "JiNao Report"

'203 Claim number	Claim Term	JiNao Report (printed publication)
	network monitors include a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	
22	The system of claim 20, wherein the plurality of domain monitors within the enterprise network interface as a plurality of peer-to-peer relationships with one another.	See '203 claim 11

Scalable Intrusion Detection for the Emerging Network "JiNao Report"

'212 Claim number	Claim Terms	JiNao Report (printed publication)
1	Method for monitoring an enterprise network, said method comprising the steps of:	See '203 claim 1
	deploying a plurality of network monitors in the enterprise network;	See '203 claim 1
	detecting, by the network monitors, suspicious network activity	See '203 claim 1
	based on analysis of network traffic data,	See '203 claim 1
	wherein at least one of the network monitors utilizes a statistical detection method;	"**2.2.1.3.1 Statistical Analysis Module** Intrusion detection using statistical analysis is founded on the contention that behavioral signatures exist for either users' usage profiles or protocol execution patterns (in this case, network routing an management protocols) and intrusion will result in abnormal signatures. Any behavior deviating from the normal signature will be considered as an anomaly and appropriate alarms can be triggered. This module provides the capability to detect intrusions that exploit previously unknown vulnerabilities." (5) [SYM_P_0070550] "**4.1.3.1 Statistical Analysis Module** In the area of computer security, statistical analysis has been reported in various projects in the literature, for example, the NIDES project at SRI [11] Wisdom and Sense at Los Alamos National Laboratory [12], and Haystack project [13] at Haystack Laboratories. Among these examples, the NIDES project at SRI is most extensive in its scope and development. It also has the most complete documentations available to the general public. With the understanding of statistical analysis's general applicability, we will adapt NIDES's statistical algorithm in our approach as a starting point and modify it as necessary.

Scalable Intrusion Detection for the Emerging Network
"JiNao Report"

'212 Claim number	Claim Term	"JiNao Report" (printed publication)
		The basic statistical approach is to compare a subject's short-term behavior with the subject's historical or long-term behavior. A subject is context-dependent, which can be a user of a computer system, a credit card holder, or one of the neighbor routers in the case of this project. In comparing short-term behavior with long-term behavior, the statistical component is concerned both with long-term behaviors that do not appear in short-term behavior, and with short-term behaviors that are not typical of long-term behavior." (18) [SYM_P_0070563] "Measures: Aspects of subject behavior are represented as measures (e.g., packet and LSA arrival frequencies in terms of their types or sources). For each measure, we will construct a probability distribution of short-term and long-term behaviors. For example, for the packet types received, the long-term probability distribution would consist of the historical probabilities with which different types of packets have been received, and the short-term probability distribution would consist of the recent probabilities with which different types [sic] packets have been received. In this case, the categories to which probabilities are attached are the names of packet types, which are learned by the system as they are received. We would classified [sic] the Ji-Nao measures into two groups: activity intensity and audit record distribution measures. These two types of measures serve different dimensional purposes. The activity measures determine whether the volume of general activity generated in the recent past (depending on the half-life of the measure, here "recent past" corresponds to the time span of last several half-lifes) is normal. These measures can detect bursts of activity or prolonged activity that is abnormal, primarily based on the volume of audit data generated. The audit record distribution measure determines whether, for recently observed activity (say, the last few hundred audit records received), the types of actions being generated across neighbors are normal. For example, we might find that the last 200 routing packets received contained 120 of Hello packets, 15 of Database Description packets, 10 of Link State Request packets, 35 of Link State Update packets, and 20 of Acknowledegment [sic] packets. These data are compared to a profile of previous activity (generated over the last few months) to determine whether or not the distribution of activity types generated in the recent past (i.e,, the last few hundred audit records) is unusual. ... For the long-term profile, the long-term aging factor is applied to the historical data at each update, and then the new information is folded in. For the short term profile, the short-term aging factor is applied to the profile with each audit record and the current audit record is folded in." (19) [SYM_P_0070564]

Scalable Intrusion Detection for the Emerging Network "JiNao Report"

'212 Claim number	'203 Claim Terms	JiNao Report (printed publication)
		"A new profile (long-term and short-term) is created whenever a new subject is first encountered." (24) [SYM_P_0070569]
	generating, by the monitors, reports of said suspicious activity; and.	See '203 claim 1
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	See '203 claim 1
2	The method of claim 1, wherein at least one of the network monitors utilizes a signature matching detection method.	"**2.2.1 Local Subsystem** A local subsystem consists of the following modules: interception/redirection module, rule-based prevention module, protocol and statistical-based detection modules, decision module, and information abstraction module." (3) [SYM_P_0070548] "**2.2.1.3.2 Protocol Analysis Module** The protocol-based approach detects intrusion by monitoring the execution of protocols in a router and triggering intrusion alarms when an anomalous state is entered. Specifically, we will investigate two routing protocols (OSPF and PNNI, the latter will be contingent upon the availability of public domain implementation of PNNI routing software) and one network management information exchange protocol (SNMP). OSPF is expected to eventually replace RIP as the primary choice of interior gateway protocol and PNNI is standardized as the routing protocol for private ATM networks. SNMP is also a standard-track Internet network management protocol. The standardization of SNMPv3 is currently work in progress at IETF. Some of the vulnerabilities of these protocols have been reported in the proposal. We continue this effort to identify potential security weaknesses and propose possible attack scenarios." (5-6) [SYM_P_0070550- SYM_P_0070551] "Similar to the case above, we will be able to dynamically modify the range of certain parameter in the statistical module or

Scalable Intrusion Detection for the Emerging Network
"JiNao Report"

'212 Claim number	Claim Items	JiNao Report (printed publication)
		import some new detecting sequences into the protocol analysis module." (9) [SYM_P_0070554] See also Section 4.1.3.2 Protocol Analysis Module (24-28) [SYM_P_0070569- SYM_P_0070573]
3	The method of claim 2, wherein the monitor utilizing a signature matching detection method also utilizes a statistical detection method.	"**2.2.1 Local Subsystem** A local subsystem consists of the following modules: interception/redirection module, rule-based prevention module, protocol and statistical-based detection modules, decision module, and information abstraction module." (3) [SYM_P_0070548]
4	The method of claim 1, wherein integrating comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2
5	The method of claim 1, wherein integrating further comprises invoking countermeasures to a suspected attack.	See '203 claim 3
6	The method of claim 1, wherein the plurality of network monitors includes an API for encapsulation of monitor	See '203 claim 4

Scalable Intrusion Detection for the Emerging Network
"JiNao Report"

'212 Claim number	Claim Terms	JiNao Report (printed publication)
	functions and integration of third-party tools.	
7	The method of claim 1, wherein the enterprise network is a TCP/IP network.	See '203 claim 5
8	The method of claim 1, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	"In this project, we focus our effort on the protection of the network infrastructure since the attacks on the routers/switches have the potential of disrupting a large scale of information services on which the national defense and economy may depend." (1) [SYM_P_0070546] "A local subsystem is associated with a router/switch to function as a security filter and analyze the incoming packets from its neighbors." (3) [SYM_P_0070548] "A JiNao local subsystem logically resides in a router or just next to it." (14) [SYM_P_0070559] "The basic statistical approach is to compare a subject's short-term behavior with the subject's historical or long-term behavior. A subject is context-dependent, which can be a user of a computer system, a credit card holder, or one of the neighbor routers in the case of this project. In comparing short-term behavior with long-term behavior, the statistical component is concerned both with long-term behaviors that do not appear in short-term behavior, and with short-term behaviors that are not typical of long-term behavior." (18) [SYM_P_0070563]
9	The method of claim 1, wherein deploying the network monitors includes placing a plurality of service	See '203 claim 8

Scalable Intrusion Detection for the Emerging Network
"JiNao Report"

'212 Claim number	Claim Term	JiNao Report (printed publication)
	monitors among multiple domains of the enterprise network.	
10	The method of claim 9, wherein receiving and integrating is performed by a domain monitor with respect to a plurality of service monitors within the domain monitor's associated network domain.	See '203 claim 8
11	The method of claim 1, wherein deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9
12	The method of claim 11, wherein receiving and integrating is performed	See '203 claim 9

Scalable Intrusion Detection for the Emerging Network "JiNao Report"

'212 Claim number	Claim Term	JiNao Report (printed publication)
	by an enterprise monitor with respect to a plurality of domain monitors within the enterprise network.	
13	The method of claim 11, wherein the plurality of the domain monitors within the enterprise network establish peer-to-peer relationships with one another.	See '203 claim 11
14	An enterprise network monitoring system comprising:	See '212 claim 1
	a plurality of network monitors deployed within an enterprise network;	See '212 claim 1
	said plurality of network monitors detecting suspicious network activity	See '212 claim 1
	based on analysis of network traffic data,	See '212 claim 1
	wherein at least one of the network monitors utilizes	See '212 claim 1

Scalable Intrusion Detection for the Emerging Network "JiNao Report"

'212 Claim Number	Claim Term	JiNao Report (printed publication)
	a statistical detection method;	
	said network monitors generating reports of said suspicious activity; and	See '212 claim 1
	one or more hierarchical monitors in the enterprise network, the hierarchical monitors adapted to automatically receive and integrate the reports of suspicious activity.	See '212 claim 1
15	The system of claim 14, wherein the integration comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2
16	The system of claim 14, wherein the integration further comprises invoking countermeasures to a suspected attack.	See '203 claim 3
17	The system of claim 14, wherein the plurality of network monitors include	See '203 claim 4

Scalable Intrusion Detection for the Emerging Network
"JiNao Report"

'212 Claim number	Claim Term	JiNao Report (printed publication)
	an application programming interface (API) for encapsulation of monitor functions and integration of third-party tools.	
18	The system of claim 14, wherein the enterprise network is a TCP/IP network.	See '203 claim 5
19	The system of claim 14, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	See '212 claim 8
20	The system of claim 14, wherein the plurality of network monitors includes a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 8
21	The system of claim 20,	See '203 claim 8

Scalable Intrusion Detection for the Emerging Network "JiNao Report"

'212 Claim number	Claim Term	JiNao Report (printed publication)
	wherein a domain monitor associated with the plurality of service monitors within the domain monitor's associated network domain is adapted to automatically receive and integrate the reports of suspicious activity.	
22	The system of claim 14, wherein the plurality of network monitors include a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9
23	The system of claim 22, wherein an enterprise monitor associated with a plurality of domain monitors is adapted to automatically receive and	See '203 claim 9

Scalable Intrusion Detection for the Emerging Network
"JiNao Report"

'212 Claim number	Claim Term	JiNao Report (printed publication)
	integrate the reports of suspicious activity.	
24	The system of claim 22, wherein the plurality of domain monitors within the enterprise network interface as a plurality of peer-to-peer relationships with one another.	See '203 claim 11

Scalable Intrusion Detection for the Emerging Network "JiNao Report"

'615 Claim number	Claim Term	JiNao Report (printed publication)
1	A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:	See '203 claim 1
	deploying a plurality of network monitors in the enterprise network;	See '203 claim 1
	detecting, by the network monitors, suspicious network activity	See '203 claim 1
	based on analysis of network traffic data selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet, network connection acknowledgements, and network packets indicative of well-known network-service protocols};	See '203 claim 1
	generating, by the monitors, reports of said suspicious activity; and	See '203 claim 1
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	See '203 claim 1
2	The method of claim 1, wherein	See '203 claim 2

Scalable Intrusion Detection for the Emerging Network
"JiNao Report"

'615 Claim number	Claim Term	JiNao Report (printed publication)
	integrating comprises correlating intrusion reports reflecting underlying commonalities.	
3	The method of claim 1, wherein integrating further comprises invoking countermeasures to a suspected attack.	See '203 claim 3
4	The method of claim 1, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4
5	The method of claim 1, wherein the enterprise network is a TCP/IP network.	See '203 claim 5
6	The method of claim 1, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	See '212 claim 8
7	The method of claim 1, wherein at least one of said network monitors utilizes a statistical detection method.	See '212 claim 1
8	The method of claim 1, wherein deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 8

Scalable Intrusion Detection for the Emerging Network "JiNao Report"

'615 Claim number	Claim Term	JiNao Report (printed publication)
9	The method of claim 8, wherein receiving and integrating is performed by a domain monitor with respect to a plurality of service monitors within the domain monitor's associated network domain.	See '203 claim 8
10	The method of claim 1, wherein deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9
12	The method of claim 10, wherein the plurality of domain monitors within the enterprise network establish peer-to-peer relationships with one another.	See '203 claim 11
13	An enterprise network monitoring system comprising:	See '615 claim 1
	a plurality of network monitors deployed within an enterprise network,	See '615 claim 1
	said plurality of network monitors detecting suspicious network activity	See '615 claim 1
	based on analysis of network traffic data selected from one or more of the following categories: {network packet data transfer commands, network packet	See '615 claim 1

Scalable Intrusion Detection for the Emerging Network "JiNao Report"

'615 Claim number	Claim Term	JiNao Report (printed publication)
	data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet, network connection acknowledgements, and network packets indicative of well-known network-service protocols};	
	said network monitors generating reports of said suspicious activity; and	See '615 claim 1
	one or more hierarchical monitors in the enterprise network, the hierarchical monitors adapted to automatically receive and integrate the reports of suspicious activity.	See '615 claim 1
14	The system of claim 13, wherein the integration comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2
15	The system of claim 13, wherein the integration further comprises invoking countermeasures to a suspected attack.	See '203 claim 3
16	The system of claim 13, wherein the plurality of network monitors include an application programming interface (API) for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4

Scalable Intrusion Detection for the Emerging Network "JiNao Report"

'615 Claim number	'615 Claim Term	JiNao Report (printed publication)
17	The system of claim 13, wherein the enterprise network is a TCP/IP network.	See '203 claim 5
18	The system of claim 13, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	See '212 claim 8
19	The system of claim 13, wherein the plurality of network monitors includes a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 8
20	The system of claim 19, wherein a domain monitor associated with the plurality of service monitors within the domain monitor's associated network domain is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 8
21	The system of claim 13, wherein the plurality of network monitors include a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9
23	The system of claim 21, wherein the	See '203 claim 11

Scalable Intrusion Detection for the Emerging Network
"JiNao Report"

'615 Claim number	Claim Term	JiNao Report (printed publication)
	plurality of domain monitors within the enterprise network interface as a plurality of peer-to-peer relationships with one another.	
34	A computer-automated method of hierarchical even monitoring and analysis within an enterprise network comprising:	See '615 claim 1
	deploying a plurality of network monitors in the enterprise network, wherein at least one of the network monitors is deployed at a gateway;	"In this project, we focus our effort on the protection of the network infrastructure since the attacks on the routers/switches have the potential of disrupting a large scale of information services on which the national defense and economy may depend." (1) [SYM_P_0070546] "A local subsystem is associated with a router/switch to function as a security filter and analyze the incoming packets from its neighbors." (3) [SYM_P_0070548] "A JiNao local subsystem logically resides in a router or just next to it." (14) [SYM_P_0070559] "The basic statistical approach is to compare a subject's short-term behavior with the subject's historical or long-term behavior. A subject is context-dependent, which can be a user of a computer system, a credit card holder, or one of the neighbor routers in the case of this project. In comparing short-term behavior with long-term behavior, the statistical component is concerned both with long-term behaviors that do not appear in short-term behavior, and with short-term behaviors that are not typical of long-term behavior." (18) [SYM_P_0070563]
	detecting, by the network monitors, suspicious network activity based on analysis of network traffic data;	See '615 claim 1
	generating, by the monitors, reports of	See '615 claim 1

Scalable Intrusion Detection for the Emerging Network "JiNao Report"

'615 Claim number	Claim Terms	JiNao Report (printed publication)
	said suspicious activity; and	
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	See '615 claim 1
35	The method of claim 34, wherein said integrating comprises correlating intrusion reports reflecting underlying commonalities.	See'203 claim 2
36	The method of claim 34, wherein said integrating further comprises invoking countermeasures to a suspected attack.	See '203 claim 3
37	The method of claim 34, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4
38	The method of claim 34, wherein said network traffic data is selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet}.	See '615 claim 1
39	The method of claim 34, wherein said	See '203 claim 7

Scalable Intrusion Detection for the Emerging Network
"JiNao Report"

'615 Claim number	Claim Term	JiNao Report (printed publication)
	deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.	
40	The method of claim 39, wherein said receiving and integrating is performed by a domain monitor with respect to a plurality of service monitors within the domain monitor's associated network domain.	See '203 claim 8
41	The method of claim 34, wherein said deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9
43	The method of claim 41, wherein the plurality of domain monitors within the enterprise network establish peer-to-peer relationships with one another.	See '203 claim 11
44	A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:	See '615 claim 1
	deploying a plurality of network monitors in the enterprise network, wherein at least	"In this project, we focus our effort on the protection of the network infrastructure since the attacks on the routers/switches have the potential of disrupting a large scale of information services on which the national

Scalable Intrusion Detection for the Emerging Network "JiNao Report"

'615 Claim number	Claim Term	JiNao Report (printed publication)
	one of the network monitors is deployed at a router;	defense and economy may depend." (1) [SYM_P_0070546] "A local subsystem is associated with a router/switch to function as a security filter and analyze the incoming packets from its neighbors." (3) [SYM_P_0070548] "A JiNao local subsystem logically resides in a router or just next to it." (14) [SYM_P_0070559] "The basic statistical approach is to compare a subject's short-term behavior with the subject's historical or long-term behavior. A subject is context-dependent, which can be a user of a computer system, a credit card holder, or one of the neighbor routers in the case of this project. In comparing short-term behavior with long-term behavior, the statistical component is concerned both with long-term behaviors that do not appear in short-term behavior, and with short-term behaviors that are not typical of long-term behavior." (18) [SYM_P_0070563]
	detecting, by the network monitors, suspicious network activity based on analysis of the network traffic data;	See '615 claim 1
	generating, by the monitors, reports of said suspicious activity; and	See '615 claim 1
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	See '615 claim 1
45	The method of claim 44, wherein said integrating comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2
46	The method of claim 44, wherein said	See '203 claim 3

Scalable Intrusion Detection for the Emerging Network "JiNao Report"

'615 Claim number	Claim Term	JiNao Report (printed publication)
	integrating further comprises invoking countermeasures to a suspected attack.	
47	The method of claim 44, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4
48	The method of claim 44, wherein said network traffic data is selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet}.	See '615 claim 1
49	The method of claim 44, wherein said deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 7
50	The method of claim 49, wherein said receiving and integrating is performed by a domain monitor with respect to a plurality of service monitors within the domain monitor's associated network	See '203 claim 8

Scalable Intrusion Detection for the Emerging Network "JiNao Report"

'615 Claim number	Claim Term	JiNao Report (printed publication)
	domain.	
51	The method of claim 44, wherein said deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9
53	The method of claim 51, wherein the plurality of domain monitors within the enterprise network establish peer-to-peer relationships with one another.	See '203 claim 11